REMARKS

In accordance with the foregoing, claim 1 has been amended. Claims 16-20 have been added. Claims 1-20 are pending and under consideration.

ALLOWABLE SUBJECT MATTER

Claims 13-15 were indicated as allowable if rewritten in independent form. Applicants acknowledge with appreciation the indication of allowable subject matter. However, since Applicants consider that claim 1, from which claims 13-15 depend, defines patentable subject matter, claims 13-15 are maintained in dependent form at the present time.

CLAIM REJECTIONS UNDER 35 U.S.C. 102

Claims 1-12 are rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,937,727 to Yup et al. (hereinafter "Yup").

On page 3, item 4 of the outstanding Office Action, the Examiner acknowledges that in the Response filed by Applicants on January 19th, 2006, Applicants argued that Yup does not teach or suggest:

- "a first selector that segments input data into execution block lengths smaller than said processing block length",
- "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length", and
- "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix Column transformation circuit."

However, in the "Response to Remarks/Arguments" section, only arguments that the first selector recited in claim 1 is anticipated by Yup are presented. The Office Action does not rebut the previously presented arguments that Yup fails to teach or suggest the intermediate register/Shift Row transformation circuit and the second selector of claim 1.

Claim 1 has been amended herewith to clarify the claimed subject matter.

In the final Office Action mailed on March 16, 2006, the Examiner indicates Yup col. 4, line 40 to col. 5, line 2 of Yup as teaching the first selector as recited in claim 1. The above-identified portion of Yup does not teach or suggest segmenting input data. In Yup, the input data is received through the input registers 102 that are coupled in the single buffer register 106. Merging "a plurality of data strings of a predetermined bit length from one of the FIFO registers 102, until a data block of a predetermined bit length is stored in the buffer register 106" is an operation opposite to "[segmenting] data into execution block lengths smaller than said processing block length."

The present invention discloses a circuit configuration that allows for a reduced circuit size while enabling high-speed processing for implementing an AES block cipher algorithm. Significant features of the invention include, but are not limited to, an intermediate register and a shift row transformation circuit that are commonly used. Additionally, the shift row transformation is only executed using a processing block length while other processes are executed using an execution block length. There is also included a second selector that selectively outputs a value from among a first selector, an intermediate register, a shift row transformation circuit, a Byte Sub transformation circuit, or a Mix Column transformation circuit. These features of the invention can be seen, for example, by an embodiment illustrated in Figure 4 of the present application.

Claim 1 recites "a second selector that outputs to said first Round Key Addition circuit one output from said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit." Yup neither teaches nor suggests this claimed limitation. In the Office Action rejection of claim 1, column 1, line 16 to column 2, line 46 in Yup allegedly discloses this claimed limitation. However, the indicated potion of Yup merely describes the generic AES block cipher algorithm without any reference to a particular hardware implementation of the AES block cipher algorithm. Yup as a whole does not teach or suggest the claimed limitation.

According the features recited in claim 1, the second selector receives input data from the first selector, the ByteSub transformation circuit, the MixColumn transformation circuit, or the intermediate register/Shift Row transformation circuit. Depending on the current processing round, the second selector is set to a different position and sends one of the above listed input values to the first Round Key Addition circuit. Yup does not teach or suggest the presence of a second selector.

Furthermore, Yup shows a circuit in which a first AddRoundKey 116, an input register

120, a ByteSub/InvByteSub 122, a ShiftRow/InvShiftRow 124, a MixCol/InvMixCol 126, and a second AddRoundKey 118 are connected in series (see Yup, FIG. 1). Because of this configuration, only the value of the second AddRoundKey 118 is stored in a storage register 110. Therefore, because of the series connection and lack of individual outputs of the ByteSub circuit 122, ShiftRow circuit 124, and the MixCol circuit 126, these individual circuits cannot provide an independent input value to the second selector even if the selector would have been included in the circuit disclosed by Yup.

Claim 1 recites individual values being inputted into the second selector. As such, Yup fails to suggest or disclose "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit."

Claim 1 further recites "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length." Yup neither teaches nor suggests this feature. As stated above, in the Office Action rejection of claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this claim limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no discussion to the particular configuration of implementing the AES block cipher algorithm as recited in claim 1 and as described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest the claimed limitation. Contrary to the present invention, Yup states that after the "initial transformation round, the data block is fed back to the cipher block input register 120 for the next transformation round" (Yup, column 6, lines 34-36). As such, Yup does not show an intermediate register that stores a value from the first Round Key Addition. Also, even though Yup discloses a storage register 110, this register is serially connected to the second Round Key Addition circuit. Therefore, it cannot receive the value from the first Round Key Addition circuit. The storage register of Yup also has no ability to perform Shift Row transformations, as recited in claim 1. As such, Yup fails to disclose "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length."

Because Yup does not disclose all the features recited in claim 1, as discussed above, it is respectfully submitted that claim 1 is patentable over the prior art. Claims 2-12 depend, directly or indirectly, from claim 1 and distinguish over the prior art at least by inheriting

patentable features from claim 1.

The circuits claimed in the present application have a reduce scale compared to prior art implementations of the AES block cipher of Rijndael. Dividing input data into execution block length segments, the execution block length being smaller than the processing block length, makes possible a reduced scale of the circuit. The Round Key Addition, Byte Sub transformation and Mix Column transformation are performed on data having execution block length.

The result of the Byte Sub transformation is stored in the intermediate register/ Shift Row transformation circuit where the Shift Row transformation is performed on data having the processing block length. In other words, the presence of a second selector makes possible according to the claimed configuration to perform Round Key Addition, Byte Sub transformation and Mix Column transformation are performed on data having execution block length although Shift Row transformation is performed on data having processing block length.

NEW CLAIMS 16-20

New independent claim 16 is directed to an encryption circuit for implementing in hardware AES. New claim 16 is fully supported by the originally filed specification and claims, for example, FIGS. 1, and 4 and original claim 1. Claim 16 is patentable at least by reciting the encryption circuit comprising "a key schedule unit that generates a plurality of round keys from a cipher key, each round key having a processing block length" and "a round function unit performing input data and round key encryption/decryption processing for each processing block length, the round function unit comprising a first selector that segments input data having processing block length into input data segments having execution block length which is smaller than said processing block length, an XOR operation unit that XORs the input data and one of the round keys and a plurality of round processing units to iterate round processing that includes Byte Sub transformation, Shift Row transformation, Mix Column transformation and Round Key Addition, wherein each round processing unit comprises a first Round Key Addition circuit that adds said round key to input data segments having said execution block length; an intermediate register/Shift Row transformation circuit that temporarily stores an output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length; a Byte Sub transformation circuit wherein a segmented output of said intermediate register/Shift Row transformation circuit is input for each said execution block length and Byte Sub transformation is executed; a second Round Key Addition circuit wherein the segmented output of said intermediate register/Shift Row transformation circuit is input for each said execution block length and said round key is added for each said execution block length; a Mix Column

transformation circuit executing Mix Column transformation on the output of said second Round Key Addition circuit; and a second selector that outputs to said first Round Key Addition circuit one output from outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix Column transformation circuit."

Dependent claims 17-20 are patentable at least by inheriting patentable from independent claim 16, but also by including additional patentable features. For example, claim 18 recites the encryption circuit further including a key expansion schedule circuit comprising a fifth selector, a shift register, a first XOR circuit, a sixth selector, a Rot Byte processing circuit, a seventh selector, a Sub Byte processing circuit, an eighth selector, a second XOR circuit, and a shift register unit selector.

CONCLUSION

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Aug. 16, 2006

By: _____
Luminita A. Todor
Registration No. 57,639

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence is being transmitted via facsimile to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on Aug. 16, 2006
STAAS & HALSEY
By: _____
Date: Aug. 16, 2006